УДК 621.396

В.А. Дмитриев, А.Б. Степанян, В.К. Фисенко
Объединенный институт проблем информатики НАН Беларуси, Беларусь
Беларусь, 220012, г. Минск, ул. Сурганова, 6

Контроль защиты конфиденциальной информации при вводе с клавиатуры ПЭВМ

U.A. Dzmitryiev, A.B. Stepanyan, U.K. Fisenko
United Institute of Informatics Problems NAS of Belarus, Belarus
Belarus, 220012, c. Minsk, Surganov str., 6

Control of Protection of Confidental Information for Input from the PC Keyboard

В.А. Дмитрієв, А.Б. Степанян, В.К. Фисенко
Об'єднаний інститут проблем інформатики НАН Білорусі, Білорусь
Білорусь, 220012, м. Мінськ, вул. Сурганова, 6

Контроль захисту конфіденційної інформації при введенні з клавіатури ПЕОМ

В статье рассмотрен метод оценки защищенности конфиденциальной информации от утечки по каналу ПЭМИ клавиатуры ПЭВМ. Данный метод основан на расчете отношения сигнал/шум, которое сравнивается с предельно допустимым отношением сигнал/шум.
Ключевые слова: защита, конфиденциальная информация, клавиатура, ПЭМИ.

An evaluation method of confidential information security from leakage via compromising emanation channel from the PC keyboard is considered. This method is based on the calculation of the signal/noise ratio which is compared to the maximum permissible signal/noise ratio.
Key words: security, confidential information, keyboard, side electromagnetic radiation.

Розглянутий метод оцінки захищеності конфіденційної інформації від витоку по каналу побічного електромагнітного випромінювання клавіатури ПЕОМ. Цей метод ґрунтується на розрахунку відношення сигнал / шум, яке порівнюється з гранично допустимим відношенням.
Ключові слова: захист, конфіденційна інформація, клавіатура,
побічне електромагнітне випромінювання.

Для оценки защищенности конфиденциальной информации от ее утечки за счет ПЭМИ клавиатуры ПЭВМ необходимо определить отношение сигнал/шум на выходе оптимального приемника (согласованного фильтра) и сравнить его с пороговым (предельным) значением. Для оценки отношения сигнал/шум используется инструментально-расчетный метод. Для измерения уровней ПЭМИ используется тестовый режим работы клавиатуры ПЭВМ. Тестовый режим должен задаваться путем формирования в клавиатуре сигнала, с одной стороны, легко идентифицируемого при приеме, а с другой – переводящего клавиатуру в состояние, при котором уровень создаваемых ею побочных излучений максимален.

Оценка возможности перехвата ПЭМИ клавиатуры ПЭВМ в открытой печати впервые была рассмотрена в [1]. Однако в этой работе не учитывались реальные условия распространения ПЭМИ клавиатуры ПЭВМ в помещении.

Наличие внутри здания стен, перегородок, мебели, радиоэлектронной аппаратуры, людей и других объектов создает сложную среду распространения радиоволн. Условия распространения ПЭМИ внутри помещений существенно отличаются от условий распространения ПЭМИ в свободном пространстве. Основными эффектами, наблюдаемыми при распространении ПЭМИ внутри помещений, являются многолучевость, обусловленная многократными отражениями радиоволн от стен и других объектов, дифракция на многочисленных острых кромках предметов, расположенных внутри комнаты, и ослабление радиоволн. Эти явления создают сложную интерференционную структуру электромагнитного излучения. Эффекты, наблюдаемые при распространении ПЭМИ, создаваемого клавиатурой компьютера, внутри помещений, приводят к быстрым замираниям амплитуды и фазы, т.е. флюктуациям сигнала ПЭМИ, приходящего к приемнику средства разведки.

Для описания статистических свойств огибающей электромагнитного излучения с быстрыми замираниями используется плотность функции m-распределения Накагами [2], которая определяется по формуле

$$G_S(U_S) = \frac{2 \cdot m^m \cdot U_S^{2 \cdot m - 1}}{\Omega_S^m \cdot \Gamma(m)} \cdot \exp\left(-\frac{m \cdot U_S^2}{\Omega_S} \right), \quad (1)$$

где $m = \dfrac{\langle U_S^2 \rangle^2}{\langle (U_S^2 - \langle U_S^2 \rangle)^2 \rangle} \geq \dfrac{1}{2}$ – глубина замираний, $\Omega_S = \langle U_S^2 \rangle = \sigma_S^2 + \langle U_S \rangle^2$, σ_S^2 – дисперсия сигнала, $\langle U_S \rangle$ – среднее значение напряжения сигнала, $\Gamma(m)$ – гамма-функция.

Статистические свойства огибающей шума описываются плотностью функции распределения Рэлея [2], которая определяется по формуле

$$G_N(U_N) = \frac{2 \cdot U_N}{\Omega_N} \cdot \exp\left(-\frac{U_N^2}{\Omega_N} \right), \quad (2)$$

где $\Omega_N = \langle U_N^2 \rangle = \sigma_N^2$, σ_N^2 – дисперсия шума.

Для оценки защищенности конфиденциальной информации от утечки по каналу ПЭМИ клавиатуры ПЭВМ необходимо рассчитать отношение сигнал/шум по напряжению на выходе оптимального приемника (согласованного фильтра) и сравнить его с пороговым (предельным) значением.

Для определения порогового (предельного) значения отношения сигнал/шум используется критерий Неймана-Пирсона, максимизирующий вероятность правильного обнаружения при заданной вероятности ложной тревоги.

При оптимальном приеме импульсного сигнала, каковым является информативный сигнал ПЭМИ клавиатуры, вероятность ошибочного приема (вероятность ложной тревоги) и вероятность правильного обнаружения одиночного импульса определяются по формулам [3]

$$P_{лт} = \int_{y_o}^{+\infty} G_N(y_N)\, dy_N = \int_{y_o}^{+\infty} G_N(U_N)\, dU_N, \quad (3)$$

$$P_o = \int_{y_o}^{+\infty} G_{S+N}(y_{S+N})\, dy_{S+N} = \int_{y_o}^{+\infty} G_{S+N}(U_{S+N})\, dU_{S+N}$$

где $P_{лт}$ – вероятность ложной тревоги, P_o – вероятность правильного обнаружения, $G_N(U_N)$ – плотность вероятности огибающей напряжения шума на входе оп-

тимального приемника, $G_{S+N}(U_{S+N})$ – плотность вероятности огибающей напряжения смеси сигнал + шум на входе оптимального приемника, y_o – пороговое значение, при превышении которого выдается решение о наличии сигнала.

Плотность вероятности огибающей напряжения смеси сигнал + шум на входе оптимального приемника определяется с помощью следующего выражения [4], [5]

$$G_{S+N}(U_{S+N}) = G_{S+N}(y_{S+N}) = \int_0^{+\infty} G_S(y_S)\cdot G_N(y_{S+N}-y_S)\,dy_S =$$

$$= X\cdot\left[y_{S+N}\cdot D_{-2\cdot m}(Z) - 2\cdot m\cdot\sqrt{\frac{\Omega_S\cdot\sigma_N^2}{2\cdot(m\cdot\sigma_N^2+\Omega_S)}}\cdot D_{-(2\cdot m+1)}(Z)\right], \qquad (5)$$

где $X = K\cdot\exp\left[-\frac{(2\cdot m\cdot\sigma_N^2+\Omega_S)}{2\cdot\sigma_N^2\cdot(m\cdot\sigma_N^2+\Omega_S)}\cdot y_{S+N}^2\right]$,

$$K = \frac{2^{2\cdot m+1}\cdot\Gamma\left(m+\frac{1}{2}\right)}{\sqrt{\pi}\cdot\sigma_N^2}\cdot\left[\frac{m\cdot\sigma_N^2}{2(m\cdot\sigma_N^2+\Omega_S)}\right]^m,$$

$$Z = -2\cdot\sqrt{\frac{\Omega_S}{2\cdot\sigma_N^2\cdot(m\cdot\sigma_N^2+\Omega_S)}}\cdot y_{S+N},$$

$D_{-B}(Z)$ – функция параболического цилиндра.

Учтя тот факт, что фаза принимаемого сигнала является случайной величиной, вероятность правильного обнаружения единичного импульса со случайной фазой рассчитывается по формуле

$$P_o = \int_{\sigma_N\cdot\sqrt{\ln\left(\frac{1}{P_{лт}}\right)}}^{+\infty} G_{S+N}(y_{S+N})\,dy_{S+N}. \qquad (6)$$

Интеграл в формуле (6) в элементарных функциях не выражается и может быть рассчитан численно, или с использованием справочных таблиц и формул. В частном случае больших отношений сигнал/шум по напряжению и небольших флуктуациях сигнала, а также используя асимптотическое значение функции параболического цилиндра [6], для вероятности правильного обнаружения единичного импульса со случайной фазой получим следующее выражение

$$P_o = \frac{m^m\cdot\Gamma\left(m+\frac{1}{2}\right)}{\sqrt{\pi}\cdot\left(q_S^2+\frac{\sigma_S^2}{\sigma_N^2}\right)^m}\cdot H, \qquad (7)$$

где $H = \Gamma\left[1-2\cdot m, \ln\left(\frac{1}{P_{лт}}\right)\right] + m\cdot\Gamma\left[-m, \ln\left(\frac{1}{P_{лт}}\right)\right]$, $\Gamma(r,x)$ – неполная гамма-функция.

Для распознавания нажимаемой клавиши клавиатуры необходимо перехватить ее скэн-код, передаваемый контроллером клавиатуры в линию передачи данных.

Полагая вероятности правильного обнаружения каждого импульса в сигнале скэн-кода независимыми, вероятность перехвата скэн-кода $P_{ск}$ можно рассчитать по формуле

$$P_{CK} = \sum_{i=1}^{n} P_{o,i} \approx \left(P_O\right)^n, \quad (8)$$

где $P_{o,i}$ – вероятность правильного обнаружения i - го импульса скэн-кода,

n – число бит (импульсов), используемых для передачи скэн-кода.

Например, в клавиатуре PS/2 для перехвата скэн-кода клавиши используется восемь бит. Поэтому, вероятность перехвата скэн-кода будет равна $P_{CK} \approx \left(P_O\right)^8$.

Задаваясь пороговым значением вероятности перехвата скэн-кода P_{CK} и вероятности ложной тревоги $P_{лт}$, можно рассчитать предельно допустимое (пороговое) значение отношения сигнал/шум δ для сигнала со случайной фазой

$$\delta \approx \sqrt{\sqrt[m]{\frac{m^m \cdot \Gamma\left(m + \frac{1}{2}\right)}{\sqrt{\pi} \cdot \sqrt[n]{P_{CK}}}} \cdot H - \frac{\sigma_S^2}{\sigma_N^2}}, \quad (9)$$

Следовательно, для оценки защищенности конфиденциально информации от утечки по каналу ПЭМИ клавиатуры ПЭВМ необходимо рассчитать отношение сигнал / шум по напряжению на выходе оптимального приемника (согласованного фильтра) q_S и сравнить его с пороговым значением δ.

Исходя из того, что для оптимального приемника полоса пропускания фильтра $\Delta F = 1/\tau$, где τ – длительность импульса, и допуская, что форма импульса прямоугольная, и полагая, что сопротивление антенны и входа приемника согласованы, q_S запишем в следующем виде

$$q_S \approx \frac{U_S}{\sigma_N \cdot \sqrt{\Delta F}},$$

где U_S – напряжение сигнала на входе разведывательного приемника, σ_N – среднеквадратическое значение напряжения шума, приведенное к входу разведывательного приемника и измеренное при полосе пропускания 1 Гц.

Конфиденциальная информация будет защищена от утечки по каналу ПЭМИ клавиатуры ПЭВМ, если $q_S < \delta$.

Литература

1. Хорев А.А. Оценка возможности перехвата побочных электромагнитных излучений клавиатуры компьютера / А.А. Хорев // Специальная техника. – 2011. – № 5. – С. 47-63.
2. Тихонов В.И. Статистическая радиотехника / Тихонов В.И. – М. : Радио и связь, 1966. – 678 с.
3. Тихонов В.И. Оптимальный прием сигналов / Тихонов В.И.. – М. : Радио и связь, 1983. – 320 с.
4. Вентцель Е.С. Теория вероятностей / Вентцель Е.С. – М.: Высшая школа, 1999. – 576 с.
5. Градштейн И.С. Таблицы интегралов, сумм, рядов и произведений / Градштейн И.С., Рыжик И.М. – М.: Физматгиз, 1963. – 1100 с.
6. Бейтмен Г. Высшие трансцендентные функции. Функции Бесселя, функции параболического цилиндра, ортогональные многочлены / Г. Бейтмен, А. Эрдейи. – М. : Наука, 1966. – Т. 2. – 296 с.

Literatura

1. Horev A.A. Evaluation of possibility of intercept of side electromagnetic radiations of computer keyboard. – Special'naja tehnika, № 5. – 2011. – S. 47-63.
2. Tihonov V.I. Statistical radio engineering. M.: A publ. is «Radio i svjaz'», 1966. – S. 678.
3. Tihonov V.I. Optimal reception of signals. M.: A publ. is «Radio i svjaz'», 1983. – S. 320.
4. Ventcel E.S. Probability theory. M.: A publ. is «Vysshaja shkola», 1999. – S. 576.
5. Gradshtejn I.S., Rygik I.M. Tables of integrals, sums, series and products. M.: A publ. is «Fizmatgiz», 1963. – S. 1100.
6. Bateman H., Erdelyi A. Higher transcendental function. M.: A publ. is «Nauka», 1966. – V. 2. – S. 296.

RESUME

U.A. Dzmitryiev, A.B. Stepanyan, U.K. Fisenko

Control of Protection of Confidental Information for Input from the PC Keyboard

In the article, the evaluation method of confidential information security from leakage via compromising emanation channel from the PC keyboard is considered. This method is based on the calculation of the signal/noise ratio which is compared to the maximum permi-sible signal/noise ratio. The received ratio is compared to a threshold (limit) signal / noise ratio. For determination of the threshold value of the signal/noise ratio the Neumann-Pearson's criterion is used, which maximizes probability of the correct detection at set probability of a false alarm.

The offered method allows to estimate the real opportunities of side electromagnetic radiation interception from the PC keyboard by means of investigation and to prove expe-diency or inexpediency of use of technical safeguards against information leakage through technical channels.

Статья поступила в редакцию 05.04.2013.